



Códigos de avaliação associados a alguns grafos bipartidos completos

Augusto Duarte Pena¹ and Cícero Fernandes de Carvalho^{†2}

¹FAMAT - Universidade Federal de Uberlândia

Palavras-chave: *Códigos parametrizados. Códigos de avaliação. Distância de Hamming generalizada.*

Resumo

Neste trabalho estudaremos códigos parametrizados por grafos bipartidos completos e suas matrizes de incidência. Utilizando algumas ferramentas de álgebra comutativa podemos calcular explicitamente o comprimento, dimensão e distância mínima destes códigos. Veremos também que, neste contexto, conseguimos uma cota superior mais refinada para os pesos de Hamming generalizados do código.

Introdução

Consideraremos \mathbb{F}_q um corpo finito com q elementos e denotaremos a cardinalidade de qualquer conjunto X por $|X|$. Seja $L = \mathbb{F}_q[Z_1, \dots, Z_n] = \bigoplus_{d \geq 0} L_d$ o anel polinomial com n variáveis. Considere o seguinte conjunto de m monômios $\mathbf{Z}^{a_1}, \dots, \mathbf{Z}^{a_m}$, onde cada $\mathbf{Z}^{a_i} = Z_1^{a_{i1}} \dots Z_n^{a_{in}}$ e a_{ij} é um inteiro não negativo para todo $i = 1, \dots, m, j = 1, \dots, n$.

Definição 1. Um **conjunto tórico parametrizado** pelos monômios acima é o seguinte subconjunto do espaço projetivo \mathbb{P}^{m-1}

$$X = \{[\mathbf{t}^{a_1} : \dots : \mathbf{t}^{a_m}] \in \mathbb{P}^{m-1} : t_i \in \mathbb{F}_q^*\}, \quad (1)$$

onde $\mathbf{t}^{a_i} = t_1^{a_{i1}} \dots t_n^{a_{in}}$, para todo $i = 1, \dots, m$, e $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$.

Além disso, consideremos $S = \mathbb{F}_q[X_1, \dots, X_m] = \bigoplus_{d \geq 0} S_d$ como outro anel de polinômios, graduado usualmente. Seja $X = \{P_1, \dots, P_{|X|}\}$ o conjunto tórico dado em (1) e consideremos a aplicação de avaliação

$$\begin{aligned} av_d : S_d &\rightarrow \mathbb{F}_q^{|X|} \\ f &\mapsto av_d(f) := \left(\frac{f(P_1)}{X_1^d(P_1)}, \dots, \frac{f(P_{|X|})}{X_1^d(P_{|X|})} \right). \end{aligned}$$

Definição 2. O **código parametrizado de ordem d** associado ao conjunto tórico X , ou o código de ordem d parametrizado pelos monômios acima, é a imagem da aplicação avaliação av_d e é denotado por $C_X(d)$. Portanto

$$C_X(d) = \left\{ \left(\frac{f(P_1)}{X_1^d(P_1)}, \dots, \frac{f(P_{|X|})}{X_1^d(P_{|X|})} \right) : f \in S_d \right\}. \quad (2)$$

Se \mathcal{B} é um subconjunto de $\mathbb{F}_q^{|X|}$, o **suporte** deste conjunto é

$$\text{supp}(\mathcal{B}) = \{i : \text{existe } (w_1, \dots, w_{|X|}) \in \mathcal{B} \text{ tal que } w_i \neq 0\}.$$

O **r -ésimo peso de Hamming generalizado** do código $C_X(d)$ é dado por

$$d_r(C_X(d)) = \min\{|\text{supp}(\mathcal{D})| : \mathcal{D} \text{ é um subcódigo de } C_X(d) \text{ e } \dim_{\mathbb{F}_q} \mathcal{D} = r\},$$

para $1 \leq r \leq H_X(d)$. A hierarquia de pesos do código $C_X(d)$ é o conjunto de inteiros $\{d_r(C_X(d)) : 1 \leq r \leq H_X(d)\}$.

Na literatura várias cotas gerais são conhecidas para diversos tipos de códigos. Em particular, estamos interessados nas seguintes cotas para as distâncias de Hamming generalizadas:

1. Cota de Singleton: $d_r(C_X(d)) \leq n - k + r$;
2. Cota de Plotkin: $d_r(C_X(d)) \leq \lfloor n(q^r - 1)q^{k-r} / (q^k - 1) \rfloor$.

^{*}augustodp@ufu.br

[†]cicero@ufu.br

O grafo bipartido completo $\mathcal{K}_{m,n}$

Um grafo G consiste em um conjunto finito não vazio V de p pontos, munido de um conjunto X com q pares ordenados de pontos distintos de V . Um grafo bipartido G é um grafo cujo conjunto V pode ser particionado em dois subconjuntos V_1 e V_2 de modo que toda aresta de G conecta V_1 com V_2 .

Seja $\mathcal{K}_{m,n}$ um grafo bipartido completo. A matriz de incidência associada a $\mathcal{K}_{m,n}$ é a matriz $B = (b_{ij})$, de ordem $(m+n) \cdot (mn)$ com $b_{ij} = 1$ se o vértice v_i e a aresta a_j são incidentes e $b_{ij} = 0$ caso contrário. Em geral, a variedade tórica X associada à matriz de incidência do grafo bipartido completo $\mathcal{K}_{m,n}$ é dada por

$$X = \{[t_1 t_{m+1} : \cdots : t_1 t_{m+n} : \cdots : t_m t_{m+1} : \cdots : t_m t_{m+n}] : t_i \in \mathbb{F}_q^* \text{ para todo } i = 1, \dots, m+n\}.$$

Escolhendo a primeira coordenada, podemos reescrever X como

$$X = \{[1 : \alpha_1 : \cdots : \alpha_{n-1} : \beta_1 : \alpha_1 \beta_1 : \cdots : \alpha_{n-1} \beta_1 : \cdots : \beta_{m-1} : \alpha_1 \beta_{m-1} : \cdots : \alpha_{n-1} \beta_{m-1}]\}.$$

Sejam

$$X_1 = \{[1 : \alpha_1 : \cdots : \alpha_{n-1}] : \alpha_1, \dots, \alpha_{n-1} \in \mathbb{F}_q^*\} \text{ e } X_2 = \{[1 : \beta_1 : \cdots : \beta_{m-1}] : \beta_1, \dots, \beta_{m-1} \in \mathbb{F}_q^*\}.$$

É claro que $|X_1| = (q-1)^{n-1}$ e $|X_2| = (q-1)^{m-1}$.

Teorema 3 ([4], Teorema 5.1). *Com a notação utilizada acima, o comprimento do código de avaliação associado à matriz de incidência do grafo bipartido completo $\mathcal{K}_{m,n}$ é dado por*

$$s = (q-1)^{m+n-2}.$$

Teorema 4 ([4], Teorema 5.2). *A dimensão do código de avaliação de ordem d associada a matriz de incidência do grafo bipartido completo $\mathcal{K}_{m,n}$ é dada por*

$$\dim_{\mathbb{F}_q} C_X(d) = H_{X_1}(d) \cdot H_{X_2}(d),$$

onde

$$\begin{aligned} H_{X_1}(d) &= \binom{n-1+d}{d} + \sum_{i=1}^{n-1} (-1)^i \binom{n-1}{i} \binom{n-1+d-i(q-1)}{d-i(q-1)} \\ &\text{e} \\ H_{X_2}(d) &= \binom{m-1+d}{d} + \sum_{i=1}^{m-1} (-1)^i \binom{m-1}{i} \binom{m-1+d-i(q-1)}{d-i(q-1)}. \end{aligned}$$

Teorema 5 ([4], Teorema 5.5). *A distância mínima do código de avaliação de ordem d associado a matriz de incidência do grafo bipartido completo $\mathcal{K}_{m,n}$, $\delta_X(d)$, é dada por*

$$\delta_X(d) = \delta_{X_1}(d) \cdot \delta_{X_2}(d).$$

Teorema 6 ([5], Teorema 4). *Seja X o conjunto tórico associado as arestas do grafo bipartido completo $\mathcal{K}_{2,n}$, com $n \geq 3$. O r -ésimo peso de Hamming generalizado do código $C_X(d)$ parametrizado por suas arestas, $1 \leq r \leq H_X(d)$ é limitado por*

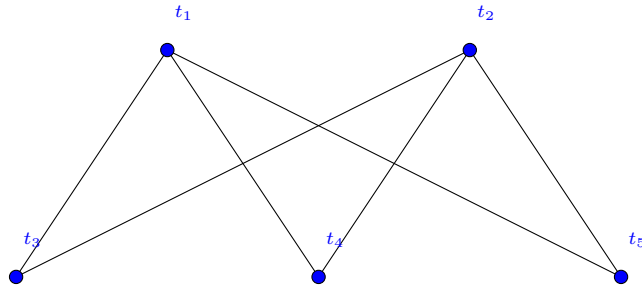
$$d_r(C_X(d)) \leq \begin{cases} (q-1)^{n-2}(q-1-d)(q+r-d-2) & \text{se } 1 \leq d \leq q-3 \\ r(q-1)^{n-(k+2)}(q-1-l) & \text{se } q-3 < d < (q-2)(n-1), \end{cases}$$

e $d_r(C_X(d)) = r$ para $d \geq (q-2)(n-1)$, onde k e l são os inteiros únicos tais que $k \geq 0$, $1 \leq l \leq q-2$ e $d = k(q-2) + l$.

Se $r = 1$ a igualdade é verificada.

Exemplo

Seja \mathbb{F}_q um corpo finito com $q = 5$ elementos e considere o grafo bipartido completo $\mathcal{K}_{2,3}$.



O conjunto tórico associado as arestas deste grafo é dado por

$$X = \{[t_1t_3 : t_1t_4 : t_1t_5 : t_2t_3 : t_2t_4 : t_2t_5] \in \mathbb{P}^5 : t_i \in \mathbb{F}_5^*\}.$$

Sua matriz de incidência é dada por

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Segue que seu comprimento é $|X| = 4^3 = 64$. A tabela a seguir dá a dimensão dos códigos correspondentes para d entre 1 e 6.

$H_X(0)$	$H_X(1)$	$H_X(2)$	$H_X(3)$	$H_X(4)$	$H_X(5)$	$H_X(6)$
1	6	18	40	52	60	64

Por fim, se tomarmos o código $C_X(3)$, sabemos que $\delta_X(3) = 4$, pois $\delta_{X_1}(3) = 4$ e $\delta_{X_2}(3) = 1$. Escolhendo $r = 3, d = 2$ como no teorema acima podemos estimar o 3-ésimo peso de Hamming do código:

$$d_3(C_X(2)) \leq 4 \cdot 2 \cdot 4 = 32.$$

Além disso $H_X(2) = 18$, logo a cota de Singleton é

$$d_3(C_X(2)) \leq |X| + 3 - H_X(2) = 4^3 + 3 - 18 = 49,$$

enquanto que a cota de Plotkin é dada por

$$d_3(C_X(2)) \leq \lfloor \frac{4^3(5^3 - 1)5^{15}}{5^{18} - 1} \rfloor = 63.$$

Portanto a cota do teorema anterior, neste caso, é melhor que ambas as cotas conhecidas.

Referências

- [1] Cícero Carvalho, *On the second Hamming weight of some Reed–Muller type codes*, Finite Fields Appl. 24. p. 88-94, 2013.
- [2] Frank Harary, *Graph Theory*, Addison-Wesley, 1971.
- [3] Joe Harris, *Algebraic Geometry: A First Course*, GTM No. 133, SpringerVerlag, Berlin, 1992.
- [4] Manuel González-Sarabia, Carlos Rentería, *Evaluation codes associated to complete bipartite graphs*, Int. J. Algebra 2. p. 163-170, 2008.
- [5] Manuel González-Sarabia, Carlos Rentería, M.A. Hernández de la Torre, *Minimum distance and second generalized Hamming weight of two particular linear codes*, Congressus Numerantium 161. p. 105-116. 2003.